(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 11 2005 001 654 T5** 2007.11.22

(12) **Veröffentlichung**

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2006/025952**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2005 001 654.4**
(86) PCT-Aktenzeichen: **PCT/US2005/024486**
(86) PCT-Anmeldetag: **08.07.2005**
(87) PCT-Veröffentlichungstag: **09.03.2006**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **22.11.2007**

(51) Int Cl.[8]: ***H04L 9/30*** (2006.01)

(30) Unionspriorität:
10/892,265 **14.07.2004** **US**

(71) Anmelder:
Intel Corp., Santa Clara, Calif., US

(74) Vertreter:
BOEHMERT & BOEHMERT, 28209 Bremen

(72) Erfinder:
Brickell, Ernest, Portland, Oreg., US; Sutton, James II., Portland, Oreg., US; Hall, Clifford, Orangevale, Calif., US; Grawrock, David, Aloha, Oreg., US

(54) Bezeichnung: **Verfahren zum Übermitteln von Direct-Proof-Privatschlüsseln an Geräte mittels einer Verteilungs-CD**

(57) Hauptanspruch: Verfahren, das umfaßt:
Erzeugen einer verschlüsselten Datenstruktur, die einer Vorrichtung zugeordnet ist, wobei die verschlüsselte Datenstruktur einen Privatschlüssel und einen Privatschlüssel-Digest umfaßt;
Erzeugen eines Kennzeichners anhand eines pseudozufällig erzeugten Werts für die verschlüsselte Datenstruktur;
Speichern des Kennzeichners und der verschlüsselten Datenstruktur auf einem entnehmbaren Speichermedium; und
Speichern des pseudozufälligen Werts in einem nichtflüchtigen Speicher in der Vorrichtung.

Beschreibung

ALLGEMEINER STAND DER TECHNIK

1. Gebiet

[0001] Die vorliegende Erfindung betrifft generell die Computersicherheit, und insbesondere das sichere Verteilen kryptographischer Schlüssel an Vorrichtungen in Verarbeitungssystemen.

2. Beschreibung

[0002] Einige Verarbeitungssystemarchitekturen, die Inhaltsschutz- und/oder Computersicherheitsfunktionen unterstützen, verlangen, daß besonders geschützte oder „vertrauenswürdige" Softwaremodule dazu in der Lage sind, eine authentifizierte, verschlüsselte Kommunikationssitzung mit besonders geschützten oder „vertrauenswürdigen" Hardwarevorrichtungen in dem Verarbeitungssystem (wie z.B. Graphiksteuerungskarten) zu herzustellen. Ein üblicherweise benutztes Verfahren sowohl zum Identifizieren der Vorrichtung als auch zum gleichzeitigen Herstellen der verschlüsselten Kommunikationssitzung besteht darin, einen einseitig authentifizierten Diffle-Helman-(DH)-Schlüsselaustauschprozeß zu benutzen. In diesem Prozeß wird der Vorrichtung ein eindeutiges Rivest-Shamir-und-Aldeman-(RSA)-Algorithmus-Schlüsselpaar oder ein eindeutiges ECC-(Elliptic Curve Cryptography – Elliptische Kurvenkryptographie)-Schlüsselpaar zugewiesen. Da jedoch dieser Authentifizierungsprozeß RSA- oder ECC-Schlüssel benutzt, weist die Vorrichtung dann eine eindeutige und belegbare Identität auf, was Anlaß zur Sorge um die Privatsphäre bereiten kann. Im schlimmsten Fall kann diese Besorgnis zu mangelnder Unterstützung durch Originalausrüstungshersteller beim Fertigen vertrauenswürdiger Vorrichtungen führen, die diese Art von Sicherheit bereitstellen.

Kurze Beschreibung der Figuren

[0003] Die Merkmale und Vorteile der vorliegenden Erfindung werden anhand der folgenden detaillierten Beschreibung der vorliegenden Erfindung deutlich, wobei:

[0004] **Fig.** 1 ein System zeigt, das eine Plattform aufweist, die mit einem TPM-(Trusted Platform Module – Vertrauenswürdiges Plattformmodul) implementiert ist, das gemäß einer Ausführungsform der Erfindung arbeitet;

[0005] **Fig.** 2 eine erste Ausführungsform der Plattform mit dem TPM aus **Fig.** 1 zeigt;

[0006] **Fig.** 3 eine zweite Ausführungsform der Plattform mit dem TPM aus **Fig.** 1 zeigt;

[0007] **Fig.** 4 ein Ausführungsbeispiel eines Computersystems zeigt, das mit dem TPM aus **Fig.** 2 implementiert ist;

[0008] **Fig.** 5 eine Darstellung eines Systems zum Verteilen von Direct-Proof-Schlüsseln gemäß einer Ausführungsform der vorliegenden Erfindung ist;

[0009] **Fig.** 6 ein Ablaufdiagramm ist, das Stufen eines Verfahrens zum Verteilen von Direct-Proof-Schlüsseln gemäß einer Ausführungsform der vorliegenden Erfindung zeigt;

[0010] **Fig.** 7 ein Ablaufdiagramm ist, das eine Einrichtungsverarbeitung bei der Vorrichtungsherstellung gemäß einer Ausführungsform der vorliegenden Erfindung zeigt;

[0011] **Fig.** 8 ein Ablaufdiagramm ist, das die Produktionsverarbeitung bei der Vorrichtungsherstellung gemäß einer Ausführungsform der vorliegenden Erfindung zeigt;

[0012] **Fig.** 9 ein Ablaufdiagramm einer Einrichtungsverarbeitung bei einem Clientcomputersystem gemäß einer Ausführungsform der Erfindung ist; und

[0013] **Fig.** 10 ein Ablaufdiagramm einer Produktionsverarbeitung bei einem Clientcomputersystem gemäß einer Ausführungsform der Erfindung ist.

DETAILLIERTE BESCHREIBUNG

[0014] Die Benutzung eines Direct-Proof-basierten Diffle-Helman-Schlüsselaustauschprotokolls, um es geschützten/vertrauenswürdigen Vorrichtungen zu erlauben, sich zu authentifizieren und eine verschlüsselte Kommunikationssitzung mit vertrauenswürdigen Softwaremodulen herzustellen, vermeidet das Erzeugen von eindeutiger Identitätsinformation in dem Verarbeitungssystem. Allerdings ist bei der direkten Einbettung eines Direct-Proof-Privatschlüssels an einer Fertigungsstraße mehr geschützter, nichtflüchtigern Speicher auf der Vorrichtung erforderlich als bei anderen Ansätzen, was die Gerätekosten in die Höhe treibt. Eine Ausführungsform der vorliegenden Erfindung ist ein Verfahren, das es dem Direct-Proof-Privatschlüssel (der z.B. zum Signieren benutzt wird) erlaubt, in einer sicheren Weise auf einem Verteiler-Compact-Disk-Lesespeicher (CD-ROM) geliefert zu werden, und anschließend von der Vorrichtung selbst in der Vorrichtung installiert zu werden. Das in dieser Erfindung vorgestellte Verfahren ist so ausgelegt, daß die Vorrichtung keine Identitätsinformation für den Installationsprozeß offenlegen muß. In einer Ausführungsform kann die Reduzierung an Vorrichtungsspeicher, der zum Unterstützen dieser Möglichkeit erforderlich ist, bei etwa 300 bis 700 Bytes bis zu etwa 20 Bytes liegen. Diese Reduzierung der Menge an nichtflüchtigem Speicher,

der zum Implementieren des Direct-Proof-basierten Diffle-Helman-Schlüsselaustauschs für Vorrichtungen benötigt wird, kann zu einer breiteren Anwendung dieses Verfahrens führen.

[0015] In der Beschreibung bedeutet die Bezugnahme auf „eine Ausführungsform" der vorliegenden Erfindung, daß ein bestimmtes Merkmal, eine Struktur oder ein Kennzeichen, die oder das im Zusammenhang mit dieser Ausführungsform beschrieben ist, in wenigstens einer Ausführungsform der vorliegenden Erfindung enthalten ist. Das Erscheinen des Ausdrucks „in einer Ausführungsform" an verschiedenen Stellen der Beschreibung bezieht sich also nicht unbedingt auf dieselbe Ausführungsform.

[0016] In der folgenden Beschreibung wird eine bestimmte Terminologie verwendet, um bestimmte Merkmale von einer oder mehreren Ausführungsformen der Erfindung zu beschreiben. Beispielsweise ist „Plattform" als jede Art von Kommunikationsgerät definiert, das dazu angepaßt ist, Information zu senden und zu empfangen. Beispiele verschiedener Plattformen sind, ohne Begrenzung oder Beschränkung darauf, Computersysteme, persönliche digitale Assistenten, Mobiltelefone, Set-Top-Boxen, Faxgeräte, Drucker, Modems, Router und ähnliches. Eine „Kommunikationsverbindung" ist im breiten Sinne als ein oder mehrere informationstragende Medien definiert, die an eine Plattform angepaßt sind. Beispiele für verschiedene Arten von Kommunikationsverbindungen sind, ohne Begrenzung oder Beschränkung darauf, elektrischer) Draht/Drähte, Lichtwellenleiter, Kabel, Bus-Trace(s) oder drahtlose Signalisierungstechnologie.

[0017] Ein „Herausforderer" bezeichnet eine Einheit (z.B. eine Person, ein System, eine Software und/oder eine Vorrichtung), die eine Verifizierung oder Authentifizierung oder Autorisierung von einer anderen Einheit verlangt. Normalerweise wird dies vor dem Offenlegen oder Bereitstellen der angeforderten Information durchgeführt. Ein „Beantworter" bezeichnet jede Einheit, von der verlangt wurde, einen Beweis ihrer Autorisierung, Gültigkeit und/oder Identität bereitzustellen. Ein „Vorrichtungshersteller", der austauschbar ist mit „zulassendem Hersteller", bezeichnet eine Einheit, die eine Plattform oder ein Gerät herstellt oder konfiguriert.

[0018] Wie hier benutzt, bedeutet das „Überzeugen" eines Herausforderers oder das „Beweisen" gegenüber einem Herausforderer, daß ein Beantworter über Kenntnisse von kryptographischer Information (z.B. einer digitalen Signatur, einem Geheimnis wie z.B. einem Schlüssel) verfügt, daß, basierend auf der Information und dem Beweis, der gegenüber dem Herausforderer offengelegt wird, eine hohe Wahrscheinlichkeit vorliegt, daß der Beantworter über die kryptographische Information verfügt. Um dies einem „Herausforderer" zu beweisen, ohne die kryptographische Information gegenüber dem Herausforderer zu „enthüllen" oder zu „offenbaren", bedeutet, daß es, basierend auf der Information, die von dem Herausforderer offenbart wird, rechnerisch unmöglich für den Herausforderer wäre, die kryptographische Information zu bestimmen.

[0019] Solche Beweise werden im Folgenden als Direct Proofs (Direktbeweise) bezeichnet. Der Begriff „Direct Proof" bezeichnet Zero-Knowledge-Beweise, da diese Arten von Beweisen auf dem Gebiet allgemein bekannt sind. Insbesondere ist ein bestimmtes Direct-Proof-Protokoll, auf das hier Bezug genommen wird, das Thema der parallelen Patentanmeldung Seriennummer 10/306,336, eingereicht am 27.11.2002, namens „System and Method for Establishing Trust Without Revealing Identity", das dem Eigentümer der vorliegenden Erfindung zugeteilt ist. Direct Proof definiert ein Protokoll, wobei ein Aussteller eine Familie mit vielen Mitgliedern festlegt, die gemeinsame Charakteristika teilen, die von dem Aussteller festgelegt werden. Der Aussteller erzeugt ein öffentliches und privates Familienschlüsselpaar (Fpub und Fpri), das die Familie insgesamt repräsentiert. Mit Hilfe von Fpri kann der Aussteller auch einen eindeutigen Direct-Proof-Privatsignaturschlüssel (DPpri) für jedes einzelne Mitglied der Familie erzeugen. Jede Nachricht, die von einem individuellen DPpri signiert wurde, kann mit Hilfe des öffentlichen Familienschlüssels Fpub verifiziert werden. Allerdings ermittelt eine solche Verifizierung nur, daß der Signierende ein Mitglied der Familie ist; es wird keine eindeutig identifizierende Information zu dem individuellen Mitglied offengelegt. In einer Ausführungsform kann der Aussteller ein Gerätehersteller oder ein Beauftragter sein. Das heißt, der Aussteller kann eine Einheit sein, die dazu in der Lage ist, anhand gemeinsamer Charakteristika Vorrichtungsfamilien zu definieren, das Öffentlich/Privat-Familienschlüsselpaar zu erzeugen, und DP-Privatschlüssel zu erzeugen und in Vorrichtungen einzubringen. Der Aussteller kann auch Zertifikate für den öffentlichen Familienschlüssel erzeugen, die die Herkunft des Schlüssels und die Kennzeichen der Vorrichtungsfamilie identifizieren.

[0020] Bezugnehmend auf **Fig.** 1 ist eine Ausführungsform eines Systems gezeigt, das eine Plattform aufweist, die mit einer vertrauenswürdigen Hardwarevorrichtung (bezeichnet als „TPM" oder „Trusted Platform Module" – Vertrauenwürdiges Plattformmodul) implementiert ist, das gemäß einer Ausführungsform der Erfindung arbeitet. Eine erste Plattform **102** (Herausforderer) überträgt eine Anfrage **106** dazu, daß eine zweite Plattform **104** (Beantworter) Information über sich selbst bereitstellt. In Antwort auf die Anfrage **106** stellt die zweite Plattform **104** die verlangte Information **108** bereit.

[0021] Zusätzlich kann es sein, daß die erste Plattform **102** für eine erhöhte Sicherheit prüfen muß, daß die verlangte Information **108** von einer Vorrichtung gekommen ist, die entweder von einem ausgewählten Vorrichtungshersteller oder einer ausgewählten Gruppe von Vorrichtungsherstellern (im Folgenden als „Vorrichtungshersteller" **110** bezeichnet) hergestellt wurde. Beispielsweise fordert in einer ersten Ausführungsform der Erfindung die erste Plattform **102** die zweite Plattform **104** heraus, zu zeigen, daß sie über kryptographische Information (z.B. eine Signatur) verfügt, die von dem/den Vorrichtungshersteller(n) **110** erzeugt wurde. Die Herausforderung kann entweder in der Anfrage **106** enthalten sein (wie dargestellt), oder in einer separaten Übertragung. Die zweite Plattform **104** antwortet auf die Herausforderung, indem sie Information in Form einer Antwort bereitstellt, um die erste Plattform **102** zu überzeugen, daß die zweite Plattform **104** über kryptographische Information verfügt, die von dem/den Vorrichtungshersteller(n) **110** erzeugt wurde, ohne die kryptographische Information zu enthüllen. Die Antwort kann entweder Teil der verlangten Information **108** sein (wie dargestellt), oder eine separate Übertragung.

[0022] In einer Ausführungsform der Erfindung umfaßt die zweite Plattform **104** ein Trusted Platform Module (TPM – Vertrauenswürdiges Plattformmodul) **115**. TPM **115** ist eine kryptographische Vorrichtung, die von dem/den Vorrichtungshersteller(n) **110** hergestellt wurde. In einer Ausführungsform der Erfindung umfaßt TPM **115** einen Prozessor mit einer geringen Menge an Chipspeicher, der in einem Paket verkapselt ist. TPM **115** ist dazu konfiguriert, Information an die erste Plattform **102** bereitzustellen, die diese in die Lage versetzt, zu bestimmen, daß eine Antwort von einem gültigen TPM übertragen wird. Die benutzte Information ist Inhalt, der es wahrscheinlich macht, daß die Identität des TPM oder der zweiten Plattform bestimmbar wird.

[0023] **Fig.** 2 zeigt eine erste Ausführungsform der zweiten Plattform **104** mit TPM **115**. Für diese Ausführungsform der Erfindung umfaßt die zweite Plattform **104** einen Prozessor **202**, der an TPM **115** gekoppelt ist. Im allgemeinen ist der Prozessor **202** eine Vorrichtung, die Information verarbeitet. Beispielsweise kann der Prozessor **202** in einer Ausführungsform der Erfindung als ein Mikroprozessor, ein Digitalsignalprozessor, eine Mikrosteuerung oder sogar ein Zustandsapparat implementiert sein. Alternativ kann der Prozessor **202** in einer anderen Ausführungsform der Erfindung als eine programmierbare oder hartcodierte Logik implementiert sein, wie z.B. als feldprogrammierbare Gate-Arrays (FPGAs), Transistor-Transistor-Logik (TTL), oder sogar als ein anwendungsspezifischer integrierter Schaltkreis (ASIC).

[0024] Hier umfaßt die zweite Plattform **104** außerdem eine Speichereinheit **206**, um die Speicherung kryptographischer Information zuzulassen, wie z.B. eine oder mehrere der folgenden: Schlüssel, Streuwerte, Signaturen, Zertifikate usw. Ein Streuwert von „X" kann als „Streu(X)" dargestellt werden. Es ist vorgesehen, daß diese Information in dem internen Speicher **220** von TPM **115** anstelle der Speichereinheit **206** gespeichert ist, wie in **Fig.** 3 gezeigt. Die kryptographische Information kann verschlüsselt sein, insbesondere wenn sie außerhalb von TPM **115** gespeichert ist.

[0025] **Fig.** 4 zeigt eine Ausführungsform einer Plattform mit einem Computersystem **300**, das mit dem TPM **115** aus **Fig.** 2 implementiert ist. Computersystem **300** umfaßt einen Bus **302** und einen Prozessor **310**, der an Bus **302** gekoppelt ist. Das Computersystem **300** umfaßt außerdem eine Hauptspeichereinheit **304** und eine statische Speichereinheit **306**.

[0026] Hier ist die Hauptspeichereinheit **304** ein flüchtiger Halbleiterspeicher zum Speichern von Information und Befehlen, die von Prozessor **310** ausgeführt werden. Der Hauptspeicher **304** kann auch dazu benutzt werden, vorläufige Variablen oder andere unmittelbare Information während der Ausführung von Befehlen durch Prozessor **310** zu speichern. Die statische Speichereinheit **306** ist ein nichtflüchtiger Halbleiterspeicher, um Information und Befehle für den Prozessor **310** dauerhafter zu speichern. Ein Beispiel eines statischen Speichers **306** ist ein Lesespeicher (ROM), ohne Beschränkung oder Begrenzung darauf. Sowohl die Hauptspeichereinheit **304** als auch die statische Speichereinheit **306** sind an Bus **302** gekoppelt.

[0027] In einer Ausführungsform der Erfindung umfaßt das Computersystem **300** außerdem eine Datenspeichervorrichtung **308**, wie z.B. eine magnetische Platte oder eine optische Platte, deren zugehöriges Laufwerk zum Speichern von Information und Befehlen auch an Computersystem **300** gekoppelt sein kann.

[0028] Computersystem **300** kann auch über Bus **302** an eine Graphiksteuerungsvorrichtung **314** gekoppelt sein, die eine Anzeige (nicht dargestellt) wie z.B. eine Kathodenstrahlröhre (KSR), eine Flüssigkristallanzeige (LCD) oder einen beliebigen Flachbildmonitor steuert, um Information für einen Endnutzer anzuzeigen. In einer Ausführungsform kann es erwünscht sein, daß die Graphiksteuerung dazu in der Lage ist, eine authentifizierte verschlüsselte Kommunikationssitzung mit einem Softwaremodul herzustellen, das von dem Prozessor ausgeführt wird.

[0029] Typischerweise kann eine alphanumerische Eingabevorrichtung **316** (z.B. Tastatur, Tastenfeld

usw.) an den Bus **302** gekoppelt sein, um Information und/oder eine Befehlauswahl an den Prozessor **310** zu übertragen. Ein anderer Typ von Nutzereingabevorrichtung ist eine Cursorsteuereinheit **318**, wie z.B. eine Maus, ein Trackball, ein integriertes Berührungsfeld, ein Taststift oder Cursorlenktasten, um Richtungsinformation und eine Befehlauswahl an den Prozessor **310** zu übertragen, und die Cursorbewegung auf der Anzeige **314** zu steuern.

[0030] Eine Kommunikationsschnittstelleneinheit **320** ist ebenfalls an den Bus **302** gekoppelt. Beispiele für eine Schnittstelleneinheit **320** sind ein Modem, eine Netzwerkschnittstellenkarte, oder andere gut bekannte Schnittstellen, die benutzt werden, um eine Kommunikationsverbindung anzuschließen, die einen Teil eines lokalen oder Weitverkehrsnetzwerks bildet. Auf diese Weise kann das Computersystem **300** über eine konventionelle Netzwerkinfrastruktur, wie z.B. das Intranet eines Unternehmens und/oder das Internet, an eine Anzahl von Clients und/oder Servern gekoppelt sein.

[0031] Man wird verstehen, daß bei bestimmten Implementierungen ein geringer oder besser ausgestattetes Computersystem als das oben beschriebene wünschenswert sein kann. Deshalb variiert die Konfigurierung des Computersystems **300** von Implementierung zu Implementierung in Abhängigkeit von zahlreichen Faktoren, wie z.B. Preisbeschränkungen, Leistungsanforderungen, technischen Verbesserungen, und/oder anderen Umständen.

[0032] In wenigstens einer Ausführungsform kann das Computersystem **300** die Benutzung besonders geschützter „vertrauenswürdiger" Softwaremodule (z.B. manipulationssicherer Software oder Systeme, die dazu in der Lage sind, geschützte Programme ablaufen zu lassen) unterstützen, die im Hauptspeicher **304** und/oder in der Massenspeichervorrichtung **308** gespeichert sind, und von dem Prozessor **310** ausgeführt werden, um spezifische Aktivitäten durchzuführen, auch in Anwesenheit von anderer feindlicher Software im System. Einige dieser vertrauenswürdigen Softwaremodule benötigen einen „vertrauenswürdigen" geschützten Zugriff, nicht nur auf eine andere Plattform, sondern auf eine oder mehrere Peripherievorrichtungen auf derselben Plattform, wie z.B. die Graphiksteuerung **314**. Im allgemeinen verlangt ein solcher Zugriff, daß das vertrauenswürdige Softwaremodul dazu in der Lage ist, die Fähigkeiten und/oder die spezifische Identität der Vorrichtung zu identifizieren, und dann eine verschlüsselte Sitzung mit der Vorrichtung herzustellen, um den Austausch von Daten zu ermöglichen, die nicht von anderer Software im System erschnüffelt oder manipuliert werden können.

[0033] Ein Verfahren des Stands der Technik, um sowohl die Vorrichtung zu identifizieren, als auch gleichzeitig die verschlüsselte Sitzung herzustellen, ist es, einen einseitigen authentifizierten Diffle-Helman-(DH)-Schlüsselaustauschprozeß zu benutzen. In diesem Prozeß wird der Vorrichtung ein eindeutiges Öffentlich/Privat-RSA- oder ECC-Schlüsselpaar zugewiesen. Die Vorrichtung enthält und schützt den Privatschlüssel, während der öffentliche Schlüssel an das Softwaremodul freigegeben werden kann. Während des DH-Schlüsselaustauschprozesses signiert die Vorrichtung mit Hilfe ihres Privatschlüssels eine Nachricht, die das Softwaremodul mit Hilfe des entsprechenden öffentlichen Schlüssels verifizieren kann. Dies erlaubt es dem Softwaremodul, zu authentifizieren, daß die Nachricht tatsächlich von der relevanten Vorrichtung stammt.

[0034] Da jedoch dieser Authentifizierungsprozeß RSA- oder ECC-Schlüssel umfaßt, weist das Gerät eine eindeutige und belegbare Identität auf. Jedes Softwaremodul, das die Vorrichtung dazu bringen kann, eine Nachricht mit ihrem privaten Schlüssel zu signieren, kann beweisen, daß diese spezifische eindeutige Vorrichtung in dem Computersystem anwesend ist. Angesichts der Tatsache, daß Vorrichtungen sich selten zwischen Verarbeitungssystemen bewegen, stellt dies auch eine belegbare eindeutige Computersystemidentität dar. Außerdem stellt der öffentliche Schlüssel der Vorrichtung selbst einen konstanten eindeutigen Wert dar; im Effekt ein permanentes „Cookie". In einigen Fällen können diese Charakteristika als ein signifikantes Privatsphärenproblem betrachtet werden.

[0035] Ein alternativer Ansatz ist in der parallelen Patentanmeldung Seriennummer 10/???,???, eingereicht am ?.?.2004, namens „An Apparatus and Method for Establishing an Authenticated Encrypted Session with a Device Without Exposing Privacy-Sensitive Information", erteilt an den Eigentümer der vorliegenden Anmeldung, beschrieben. In diesem Ansatz wird die Benutzung von RSA- oder ECC-Schlüsseln in dem einseitig authentifizierten Diffle-Helman-Prozeß durch Direct-Proof-Schlüssel ersetzt. Eine einseitigen, authentifiziert, die diesen Ansatz benutzt, kann als zu einer spezifischen Vorrichtungsfamilie zugehörig authentifiziert werden, was Versicherungen zum Verhalten oder zur Vertrauenswürdigkeit der Vorrichtung mit einschließen kann. Der Ansatz gibt keine eindeutig identifizierende Information frei, die benutzt werden könnte, um eine eindeutige Identität aufzustellen, die das Verarbeitungssystem darstellt.

[0036] Obwohl der Ansatz gut funktioniert, benötigt er zusätzlichen Speicher in der Vorrichtung, um den Direct-Proof-Privatschlüssel aufzunehmen, der größer sein kann als ein RSA- oder ECC-Schlüssel. Um die Belastung durch diesen zusätzlichen Speicherbedarf zu senken, definieren Ausführungsformen der vorliegenden Erfindung ein System und einen Pro-

zeß, um sicherzustellen, daß die Vorrichtung über den Direct-Proof-Privatschlüssel verfügt, wenn sie den Schlüssel benötigt, ohne daß eine wesentliche Menge zusätzlichen Speichers in der Vorrichtung benötigt wird.

[0037] In wenigstens einer Ausführungsform der vorliegenden Erfindung speichert ein Vorrichtungshersteller an der Fertigungsstraße nur eine pseudozufällige 128-Bit-Zahl in einer Vorrichtung, wobei ein wesentlich größerer Direct-Proof-Privatschlüssel (DPpri) unter Benutzung einer Verteiler-CD verschlüsselt und geliefert werden kann. Andere Ausführungsformen können eine Zahl in der Vorrichtung speichern, die länger oder kürzer als 128 Bits ist. Dieser Prozeß stellt sicher, daß nur eine spezifizierte Vorrichtung ihren zugewiesenen DPpri-Schlüssel entschlüsseln und benutzen kann. **Fig.** 5 ist eine Darstellung eines Systems **500** zum Verteilen von Direct-Proof-Schlüsseln gemäß einer Ausführungsform der vorliegenden Erfindung. In dem System liegen drei Einheiten vor, ein geschütztes Vorrichtungsherstellungssystem **502**, ein Vorrichtungsherstellungs-Produktionssystem **503**, und ein Clientcomputersystem **504**. Das geschützte Vorrichtungsherstellungssystem umfaßt ein Verarbeitungssystem, das im Einrichtungsprozeß vor dem Herstellen einer Vorrichtung **506** benutzt wird. Das geschützte System **502** kann von einem Vorrichtungshersteller so betrieben werden, daß das geschützte System vor einem Angriff durch Hacker außerhalb des Vorrichtungsherstellungsstandorts geschützt ist (z.B. in einem geschlossenen System). Das Herstellungsproduktionssystem **503** kann bei der Herstellung der Vorrichtungen benutzt werden. In einer Ausführungsform können das geschützte System und das Produktionssystem dasselbe System sein. Die Vorrichtung **506** umfaßt jede Hardwarevorrichtung, die in das Clientcomputersystem aufzunehmen ist (z.B. eine Speichersteuerung, eine Peripherievorrichtung wie z.B. eine Graphiksteuerung, ein E/A-Vorrichtung usw.). In Ausführungsformen der vorliegenden Erfindung umfaßt die Vorrichtung einen pseudozufälligen Wert RAND **508**, der in einem nichtflüchtigen Speicher der Vorrichtung gespeichert ist.

[0038] Das geschützte Herstellungssystem beinhaltet eine geschützte Datenbank **510** und eine Erzeugungsfunktion **512**. Die geschützte Datenbank umfaßt eine Datenstruktur, um eine Vielzahl pseudozufälliger Werte zu speichern (wenigstens so viele, wie herzustellende Vorrichtungen vorliegen), die von der Erzeugungsfunktion **512** in einer unten beschriebenen Weise erzeugt werden. Die Erzeugungsfunktion umfaßt Logik (entweder in Software oder Hardware implementiert) zum Erzeugen einer Datenstruktur, die hier als Keyblob **514** bezeichnet wird. Der Keyblob **514** umfaßt wenigstens drei Datenobjekte. Ein eindeutiger Direct-Proof-Privatschlüssel (DPpri) umfaßt einen kryptographischen Schlüssel, der von einer Vorrichtung zum Signieren benutzt werden kann. Der DP-Privat-Digest **516** (dppri-Digest) umfaßt einen Nachrichten-Digest, wie z.B. SHA-1. Einige Ausführungsformen können einen pseudozufälligen Initialisierungsvektor (IV) **518** beinhalten, der zu Kompatibilitätszwecken einen Bitstrom als Teil des Keyblobs umfaßt. Wenn für die Verschlüsselung ein Stromchiffre benutzt wird, dann wird der IV in einem gut bekannten Verfahren zum Benutzen eines IV in einem Stromchiffre benutzt. Wenn für die Verschlüsselung ein Blockchiffre benutzt wird, wird der IV als Teil der zu verschlüsselnden Nachricht benutzt, was jede Instanz der Verschlüsselung unterschiedlich gestaltet.

[0039] In Ausführungsformen der vorliegenden Erfindung erzeugt das geschützte Herstellungssystem einen oder mehrere Keyblobs (wie weiter unten im Detail beschrieben), und speichert die Keyblobs in einer Keyblob-Datenbank **520** auf einer CD **522**. In einer Ausführungsform können sich auf einer einzigen CD viele Keyblobs befinden, wobei die Speicherbegrenzung der CD die einzige Beschränkung ist. Die CD wird dann über typische physikalische Kanäle an Computersystemhersteller, Computerhändler, Verbraucher und andere verteilt. Obwohl hier eine CD als das Speichermedium beschrieben ist, kann jedes geeignete entnehmbare Speichermedium benutzt werden (z.B. eine DVD (digital versatile disk) oder ein anderes Medium).

[0040] Ein Clientcomputersystem **504**, das ein Direct-Proof-Protokoll zur Authentifizierung und zum Schlüsselaustausch einer Kommunikationssitzung mit Vorrichtung **506** benutzen möchte, die in dem System **504** enthalten ist, kann einen ausgewählten Keyblob **514** aus der Keyblob-Datenbank **520** von der CD ablesen, sobald die CD in ein CDROM-Laufwerk (nicht dargestellt) des Clientcomputersystems eingeführt wurde. Die Keyblob-Daten können von der Vorrichtung benutzt werden, um einen lokalisierten Keyblob **524** zu erzeugen (wie unten beschrieben), der zum Implementieren des Direct-Proof-Protokolls benutzt wird. Eine Vorrichtungstreibersoftware **526** wird von dem Clientcomputersystem ausgeführt, um Vorrichtung **506** zu initialisieren und zu steuern.

[0041] In Ausführungsformen der vorliegenden Erfindung können vier klar abgegrenzte Operationsstufen vorliegen. **Fig.** 6 ist ein Ablaufdiagramm **600**, das Stufen eines Verfahrens zum Verteilen von Direct-Proof-Schlüsseln gemäß einer Ausführungsform der vorliegenden Erfindung zeigt. Gemäß Ausführungsformen der vorliegenden Erfindung können auf jeder Stufe bestimmte Handlungen ausgeführt werden. An einem Standort des Herstellers finden wenigstens zwei Stufen statt: die Einrichtungsstufe **602** und die Herstellungsproduktionsstufe **604**.

[0042] Die Einrichtungsstufe ist hier unter Bezugnahme auf **Fig.** 7 beschrieben. Die Herstellungspro-

duktionsstufe ist hier unter Bezugnahme auf **Fig.** 8 beschrieben. Am Standort des Verbrauchers, der das Clientcomputersystem besitzt, finden wenigstens zwei Stufen statt: die Einrichtungsstufe **606** und die Benutzungsstufe **608**. Die Einrichtungsstufe im Clientcomputersystem ist hier unter Bezugnahme auf **Fig.** 9 beschrieben. Die Benutzungsstufe im Clientcomputersystem ist hier unter Bezugnahme auf **Fig.** 10 beschrieben.

[0043] **Fig.** 7 ist ein Ablaufdiagramm **700**, das die Einrichtungsverarbeitung bei der Vorrichtungsherstellung gemäß einer Ausführungsform der vorliegenden Erfindung zeigt. In einer Ausführungsform kann ein Vorrichtungshersteller diese Handlungen mit Hilfe eines geschützten Herstellungssystems **502** durchführen. An Block **702** erzeugt der Vorrichtungshersteller ein Direct-Proof-Familienschlüsselpaar (Fpub und Fpri) für jede herzustellende Vorrichtungsklasse. Jede einzelne Vorrichtung weist einen DPpri-Schlüssel auf, so daß eine Signatur, die unter Benutzung von DPpri erzeugt wird, durch Fpub verifiziert werden kann. Eine Klasse von Vorrichtungen kann jede Menge oder Untermenge von Vorrichtungen umfassen, wie z.B. eine ausgewählte Produktlinie (z.B. einen Typ Vorrichtung), oder Untermengen einer Produktlinie, basierend auf Versionsnummer, oder auf anderen Charakteristika der Vorrichtungen. Das Familienschlüsselpaar dient der Benutzung durch die Klasse von Vorrichtungen, für die es erzeugt wurde.

[0044] Für jede herzustellende Vorrichtung führt die Erzeugungsfunktion **512** des geschützten Herstellungssystems **502** die Blöcke **704** bis **720** durch. Zunächst erzeugt die Erzeugungsfunktion an Block **704** einen eindeutigen pseudozufälligen Wert (RAND) **508**. In einer Ausführungsform beträgt die Länge von RAND 128 Bits. In anderen Ausführungsformen können andere Wertgrößen benutzt werden. In einer Ausführungsform können die pseudozufälligen Werte für eine Anzahl von Vorrichtungen im Voraus erzeugt werden. An Block **706** erzeugt die Erzeugungsfunktion unter Benutzung einer Einwegfunktion f, unterstützt durch die Vorrichtung, einen symmetrischen Verschlüsselungsschlüssel SKEY aus dem eindeutigen RAND-Wert (SKEY = f(RAND)). Die Einwegfunktion kann jeder bekannte Algorithmus sein, der zu diesem Zweck geeignet ist (z.B. SHA-1, MGF1, Data Encryption Standard (DES), Triple-DES usw.). An Block **708** erzeugt die Erzeugungsfunktion in einer Ausführungsform eine Kennzeichner-(ID)-Markierung, die benutzt wird, um auf der Verteiler-CD **522** auf den Keyblob **514** dieser Vorrichtung zu verweisen, indem SKEY zum Verschlüsseln eines „Nulleintrags" benutzt wird (z.B. eine kleine Zahl von Null-Bytes)(Vorrichtungs-ID = Verschlüssselung (0..0) mit SKEY). In anderen Ausführungsformen können andere Verfahren zum Erzeugen der Vorrichtungs-ID benutzt werden, oder es können andere Werte von SKEY verschlüsselt werden.

[0045] Als nächstes erzeugt die Erzeugungsfunktion an Block **710** den DP-Privatsignaturschlüssel DPpri, der mit dem öffentlichen Familienschlüssel (Fpub) der Vorrichtung korreliert. An Block **712** streut die Erzeugungsfunktion DPpri, um unter Benutzung bekannter Verfahren einen DPpri-Digest zu erstellen (z.B. unter Benutzung von SHA-1 oder einem anderen Streuwertalgorithmus). An Block **714** erstellt die Erzeugungsfunktion eine Keyblob1-Datenstruktur für die Vorrichtung. Der Keyblob enthält wenigstens DPpri und DPpri-Digest. In einer Ausführungsform enthält der Keyblob auch einen zufälligen Initialisierungsvektor, der mehrere pseudozufällig erzeugte Bits aufweist. Diese Werte können unter Benutzung von SKEY verschlüsselt werden, um einen verschlüsselten Keyblob **514** zu erstellen. An Block **716** können die Vorrichtungs-ID, die an Block **708** erzeugt wurde, und der verschlüsselte Keyblob **514**, der an Block **714** erzeugt wurde, in einem Eintrag in einer Keyblob-Datenbank **520** gespeichert werden, die auf der Verteiler-CD **522** freigegeben wird. In einer Ausführungsform kann der Eintrag in der Keyblob-Datenbank von der Vorrichtungs-ID angezeigt werden. An Block **718** kann der aktuelle RAND-Wert in der geschützten Datenbank **510** gespeichert werden. An Block **720** können SKEY und DPpri gelöscht werden, da sie durch die Vorrichtung im Feld regeneriert werden. Die Erzeugung des DPpri-Digests und die anschließende Verschlüsselung durch SKEY sind so ausgelegt, daß der Inhalt von DPpri nicht durch eine Einheit bestimmt werden kann, die nicht in Besitz von SKEY ist, und so, daß der Inhalt des KeyBlob nicht von einer Einheit verändert werden kann, die nicht in Besitz von SKEY ist, ohne daß dies anschließend von einer Einheit entdeckt wird, die in Besitz von SKEY ist. In anderen Ausführungsformen können andere Verfahren zum Bereitstellen der Geheimhaltung und zum Schutz der Unversehrtheit benutzt werden. In einigen Ausführungsformen kann es sein, daß der Unversehrtheitsschutz nicht erforderlich ist, und es kann ein Verfahren benutzt werden, das nur eine Geheimhaltung bereitstellt. In diesem Fall wäre der Wert von DPpri-Digest nicht nötig.

[0046] Zu jedem Zeitpunkt nach Block **720** kann an Block **720** die geschützte Datenbank von RAND-Werten sicher in das Herstellungsproduktionssystem **503** geladen werden, das die RAND-Werte während des Herstellungsprozesses in den Vorrichtungen speichert. Nachdem dieser Ladevorgang verifiziert wurde, können die RAND-Werte sicher aus dem geschützten Herstellungssystem **502** gelöscht werden. Zuletzt kann an Block **724** die Keyblob-Datenbank, die mehrere verschlüsselte Keyblobs aufweist, auf eine übliche Verteiler-CD **522** „gebrannt" werden. In einer Ausführungsform kann die CD zusammen mit der Vorrichtung verteilt werden, wobei für jede Vorrichtung ein Keyblob-Datenbankeintrag

benutzt wird, wie in dem Vorrichtungs-ID-Feld indexiert. Außerdem weist die CD ein Dienstprogrammsoftwaremodul zur Schlüsselrückholung auf, dessen Benutzung im Folgenden genauer beschrieben werden soll.

[0047] **Fig.** 8 ist ein Ablaufdiagramm **800**, das die Produktionsverarbeitung bei der Vorrichtungsherstellung gemäß einer Ausführungsform der vorliegenden Erfindung darstellt. Während an einer Fertigungsstraße Vorrichtungen hergestellt werden, wählt das Herstellungsproduktionssystem bei Block **802** einen ungenutzten RAND-Wert aus der geschützten Datenbank aus. Der ausgewählte RAND-Wert kann dann in einem nichtflüchtigen Speicher in einer Vorrichtung gespeichert werden. In einer Ausführungsform umfaßt der nichtflüchtige Speicher ein TPM. An Block **804** zerstört das Herstellungsproduktionssystem nach erfolgreicher Speicherung des RAND-Werts jede Aufzeichnung des RAND-Werts der Vorrichtung in der geschützten Datenbank. An diesem Punkt ist die einzige Kopie des RAND-Werts in der Vorrichtung gespeichert.

[0048] In einer alternativen Ausführungsform kann der RAND-Wert während der Herstellung einer Vorrichtung erzeugt werden, und wird dann an das geschützte Herstellungssystem gesendet, um einen Keyblob zu berechnen.

[0049] In einer anderen Ausführungsform kann der RAND-Wert auf der Vorrichtung erzeugt werden, und die Vorrichtung und das geschützte Herstellungssystem können in ein Protokoll eintreten, um den DPpri-Schlüssel zu erzeugen, wobei ein Verfahren benutzt wird, das den DPpri-Schlüssel nicht außerhalb des Keyblob offenlegt. Die Vorrichtung leitet die Vorrichtungs-ID und den Keyblob zum Speichern in der geschützten Datenbank **510** an das Herstellungssystem weiter. In diesem Verfahren weist das Herstellungssystem letztlich dieselbe Information (Vorrichtungs-ID, Keyblob) in der geschützten Datenbank auf, kennt jedoch die Werte von RAND oder von DPpri nicht.

[0050] **Fig.** 9 ist ein Ablaufdiagramm **900** einer Einrichtungsverarbeitung bei einem Clientcomputersystem gemäß einer Ausführungsform der vorliegenden Erfindung. Ein Clientcomputersystem kann diese Handlungen als Teil des Systemstarts durchführen. An Block **902** kann das Clientcomputersystem in normaler Weise hochgefahren werden, und ein Vorrichtungstreiber **526** für die Vorrichtung kann in den Hauptspeicher geladen werden. Wenn der Vorrichtungstreiber initialisiert wurde und mit der Ausführung beginnt, bestimmt die Vorrichtung, ob bereits ein verschlüsselter lokalisierter Keyblob **524** in der Massenspeichervorrichtung **308** für Vorrichtung **506** gespeichert ist. Wenn ja, muß keine weitere Einrichtungsverarbeitung durchgeführt werden, und die Einrichtungsverarbeitung endet an Block **906**. Wenn nicht, fährt die Einrichtungsverarbeitung an Block **908** fort. An Block **908** veranlaßt der Vorrichtungstreiber die Anzeige der Nachricht an den Nutzer des Clientcomputersystems, und bittet um die Verteiler-CD **522**. Wenn die CD vom Computersystem eingelesen wurde, startet der Vorrichtungstreiber die Dienstprogrammsoftware zur Schlüsselrückholung (in **Fig.** 5 nicht gezeigt), die auf der CD gespeichert ist. Dieses Dienstprogramm stellt ein Befehl zum Erhalten des Schlüssels an die Vorrichtung **506** aus, um den Prozeß des DP-Privatschlüsselerhalts von der Vorrichtung einzuleiten.

[0051] In Antwort darauf benutzt die Vorrichtung an Block **910** ihre Einwegfunktion f, um den symmetrischen Schlüssel SKEY (jetzt zur Benutzung bei der Entschlüsselung) aus dem eingebetteten RAND-Wert **508** zu regenerieren (SKEY = F(RAND)). An Block **912** erzeugt die Vorrichtung dann ihre eindeutige Vorrichtungs-ID-Markierung, indem SKEY benutzt wird, um einen „Null-eintrag" zu verschlüsseln (z.B. eine kleine Anzahl von Null-Bytes)(Vorrichtungs-ID = Verschlüsselung (0..0) mit SKEY). Die Vorrichtung gibt dann die Vorrichtungs-ID an die Dienstprogrammsoftware zur Schlüsselrückholung zurück. An Block **914** durchsucht das Schlüsselrückholungsdienstprogramm die Keyblob-Datenbank **520** auf der CD nach dem Datenbankeintrag, der die passende Vorrichtungs-ID enthält, extrahiert den verschlüsselten Keyblob der Vorrichtung, und überträgt den Keyblob an die Vorrichtung.

[0052] In einer Ausführungsform antwortet die Vorrichtung, wenn Rogue-Software versucht, ein Schlüsselerhaltsbefehl an die Vorrichtung zu senden, nachdem die Vorrichtung den Keyblob erhalten hat, nicht mit der Vorrichtungs-ID auf die Rogue-Software. Statt dessen gibt die Vorrichtung eine Fehleranzeige zurück. Im Effekt wird die Funktion des Schlüsselerhaltsbefehls deaktiviert, wenn die Vorrichtung über Zugriff auf einen lokalisierten Keyblob verfügt. Auf diese Weise enthüllt die Vorrichtung die eindeutige Vorrichtungs-ID nicht, es sei denn, sie verfügt nicht über den Keyblob.

[0053] An Block **916** entschlüsselt die Vorrichtung den verschlüsselten Keyblob unter Benutzung des symmetrischen Schlüssels SKEY, um DPpri und DPpri-Digest zu erhalten, und speichert diese Werte in ihrem nichtflüchtigen Speicher (Entschlüsselter Keyblob = Entschlüsselung (IV, DPpri, DPpri-Digest) mit SKEY). Der Initialisierungsvektor (IV) kann verworfen werden. An Block **918** prüft die Vorrichtung dann die Unversehrtheit von DPpri durch Streuen von DPpri und durch Vergleichen des Ergebnisses mit DPpri-Digest. Wenn der Vergleich gut ist, akzeptiert die Vorrichtung DPpri als ihren gültigen Schlüssel. Die Vorrichtung kann auch einen Schlüsselerhalten-Bitschalter auf wahr setzen, um anzuzeigen, daß

der DP-Privatschlüssel erfolgreich erhalten wurde. An Block **920** wählt die Vorrichtung einen neuen IV, und erzeugt einen neuen verschlüsselten lokalisierten Keyblob, unter Benutzung des neuen IV (Lokalisierter Keyblob = Verschlüsselung (IV2, DPpri, DPpri-Digest) mit SKEY). Der neue verschlüsselte lokalisierte Keyblob kann an das Dienstprogramm zur Schlüsselrückholung zurückgegeben werden. An Block **922** speichert das Dienstprogramm zur Schlüsselrückholung den verschlüsselten, lokalisierten Keyblob im Speicher in dem Clientcomputersystem (wie z.B. in der Massenspeichervorrichtung **308**). Der DPpri der Vorrichtung ist nun sicher im Clientcomputersystem gespeichert.

[0054] Sobald die Vorrichtung während der Einrichtungsverarbeitung DPpri erhalten hat, kann die Vorrichtung dann DPpri benutzen. **Fig.** 10 ist ein Ablaufdiagramm einer Clientcomputersystemverarbeitung gemäß einer Ausführungsform der vorliegenden Erfindung. Das Clientcomputersystem kann diese Handlungen jederzeit nach Abschluß der Einrichtung durchführen. An Block **1002** kann das Clientcomputersystem auf normale Weise hochgefahren werden, und ein Vorrichtungstreiber **526** für die Vorrichtung kann in den Hauptspeicher geladen werden. Wenn der Vorrichtungstreiber initialisiert ist und mit der Ausführung beginnt, bestimmt der Vorrichtungstreiber, ob bereits ein verschlüsselter lokalisierter Keyblob **524** in der Massenspeichervorrichtung **308** für Vorrichtung **506** gespeichert ist. Wenn ein verschlüsselter lokalisierter Keyblob für diese Vorrichtung verfügbar ist, fährt die Verarbeitung an Block **1006** fort. An Block **1006** holt der Vorrichtungstreiber den verschlüsselten lokalisierten Keyblob zurück, und überträgt den Keyblob an die Vorrichtung. In einer Ausführungsform kann die Übertragung des Keyblob durch Ausführen eines Keyblob-Ladebefehls erreicht werden.

[0055] An Block **1008** benutzt die Vorrichtung ihre Einwegfunktion f, um den symmetrischen Schlüssel SKEY (der nun zur Entschlüsselung benutzt wird) aus dem eingebetteten RAND-Wert **508** zu regenerieren (SKEY = f(RAND)). An Block **1010** entschlüsselt die Vorrichtung den verschlüsselten lokalisierten Keyblob unter Benutzung des symmetrischen Schlüssels SKEY, um DPpri und DPpri-Digest zu erhalten, und speichert diese Werte in ihrem nichtflüchtigen Speicher (Entschlüsselter Keyblob = Entschlüsselung (IV2, DPpri, DPpri-Digest) mit SKEY). Der zweite Initialisierungsvektor (IV2) kann verworfen werden. An Block **1012** prüft die Vorrichtung die Unversehrtheit von DPpri durch Streuen von DPpri und durch Vergleichen des Ergebnisses mit DPpri-Digest. Wenn der Vergleich gut ist (z.B. wenn die Digests übereinstimmen), akzeptiert die Vorrichtung DPpri als den zuvor erhaltenen gültigen Schlüssel, und aktiviert ihn zur Benutzung. Die Vorrichtung kann auch den Schlüssel-erhalten-Bitschalter auf wahr setzen, um anzuzeigen, daß der DP-Privatschlüssel erfolgreich erhalten wurde. An Block **1014** wählt die Vorrichtung einen weiteren IV, und erzeugt einen neuen lokalisierten Keyblob, unter Benutzung des neuen IV (Lokalisierter Keyblob = Verschlüsselung (IV3, DPpri, DPpri-Digest) mit SKEY). Der neue verschlüsselte lokalisierte Keyblob kann an das Dienstprogramm zur Schlüsselrückholung zurückgegeben werden. An Block **1016** speichert das Dienstprogramm zur Schlüsselrückholung den verschlüsselten, lokalisierten Keyblob im Speicher im Clientcomputersystem (wie z.B. der Massenspeichervorrichtung **308**). Der DPpri der Vorrichtung ist nun wieder sicher in dem Clientcomputersystem gespeichert.

[0056] In einer Ausführungsform der vorliegenden Erfindung ist es nicht nötig, alle DP-Privatschlüssel der Vorrichtung zugleich zu erzeugen. Unter der Annahme, daß die Verteiler-CD regelmäßig aktualisiert wird, können die DP-Privatschlüssel der Vorrichtung nach Bedarf stoßweise erzeugt werden. Jedesmal, wenn eine Verteiler-CD „gebrannt" wird, enthält sie die zum aktuellen Zeitpunkt erzeugte Keyblob-Datenbank, einschließlich derjenigen Vorrichtungsschlüssel, die bereits erzeugt wurden, aber den Vorrichtungen noch nicht zugeordnet wurden.

[0057] Obwohl die hier erörterten Operationen als ein sequentieller Prozeß beschrieben werden können, können einige der Operationen tatsächlich parallel oder aufeinander folgend ausgeführt werden. Außerdem kann in einigen Ausführungsformen die Abfolge der Operationen umgestellt werden, ohne vom Geist der Erfindung abzuweichen.

[0058] Die hier beschriebenen Verfahren sind nicht auf eine bestimmte Hardware- oder Softwarekonfigurierung beschränkt; sie können in jeder Rechen- oder Verarbeitungsumgebung Anwendung finden. Die Verfahren können in Hardware, Software oder einer Kombination der beiden implementiert werden. Die Verfahren können in Programmen implementiert werden, die auf programmierbaren Maschinen ausführen, wie z.B. mobilen oder stationären Computern, persönlichen digitalen Assistenten, Set-Top-Boxen, Mobiltelefonen und Pagern, und anderen elektronischen Vorrichtungen, die jeweils einen Prozessor, ein von dem Prozessor lesbares Speichermedium (einschließlich flüchtiger und nichtflüchtiger Speicherelemente), wenigstens eine Eingabevorrichtung, und eine oder mehrere Ausgabevorrichtungen aufweisen. Die Ausgabeinformation kann auf eine oder mehrere Ausgabevorrichtungen angewandt werden. Ein Durchschnittsfachmann wird verstehen, daß die Erfindung mit verschiedenen Computersystemkonfigurierungen praktizierbar ist, darunter Multiprozessorsystemen, Minicomputern, Großrechnern und ähnlichem. Die Erfindung kann auch in verteilten Computerumgebungen praktiziert werden, in denen Aufgaben von entfernten Vorrichtungen durchgeführt wer-

den, die über ein Kommunikationsnetzwerk verbunden sind.

[0059] Jedes Programm kann in einer verfahrensorientierten oder objektorientierten Programmiersprache der höheren Ebene implementiert sein, um mit einem Verarbeitungssystem zu kommunizieren. Allerdings können Programme nach Bedarf in Assembler- oder Maschinensprache implementiert sein. Auf jeden Fall kann die Sprache kompiliert oder interpretiert werden.

[0060] Programmbefehle können dazu benutzt werden, ein allgemeines oder für einen spezifischen Zweck bestimmtes Verarbeitungssystem hervorzurufen, das mit den Befehlen programmiert wird, um die hier beschriebenen Operationen durchzuführen. Alternativ können die Operationen mit spezifischen Hardwarekomponenten durchgeführt werden, die hartverdrahtete Logik zum Durchführen der Operationen enthalten, oder durch jede beliebige Kombination programmierter Computerkomponenten und angepaßter Hardwarekomponenten. Die hier beschriebenen Verfahren können als ein Computerprogrammprodukt bereitgestellt werden, das ein maschinenlesbares Medium beinhalten kann, auf dem Befehle gespeichert sind, die benutzt werden können, um ein Verarbeitungssystem oder eine andere elektronische Vorrichtung zu programmieren, um die Verfahren durchzuführen. Der hier benutzte Begriff „maschinenlesbares Medium" beinhaltet jedes Medium, das dazu in der Lage ist, eine Sequenz von Befehlen zu speichern oder zu codieren, die zur Ausführung durch die Maschine vorgesehen sind, und das die Maschine veranlassen kann, eines der hier beschriebenen Verfahren auszuführen. Der Begriff „maschinenlesbares Medium" beinhaltet entsprechend, ohne Beschränkung darauf, Halbleiterspeicher, optische und magnetische Platten, und eine Trägerwelle, die ein Datensignal codiert. Außerdem ist es auf dem Gebiet üblich, von Software in der einen oder anderen Form (z.B. als Programm, Verfahren, Prozeß, Anwendung, Modul, Logik usw.) als eine Handlung durchführend oder ein Ergebnis verursachend zu sprechen. Derartige Ausdrücke sind lediglich eine verkürzte Art, auszudrücken, daß die Ausführung der Software durch ein Verarbeitungssystem den Prozessor dazu veranlaßt, eine Handlung durchzuführen oder ein Ergebnis zu erzeugen.

[0061] Obwohl diese Erfindung unter Bezugnahme auf erläuternde Ausführungsformen beschrieben wurde, ist diese Beschreibung nicht in begrenzendem Sinne zu verstehen. Verschiedene Modifikationen veranschaulichender Ausführungsformen, sowie andere Ausführungsformen, die einem Fachmann auf dem Gebiet der Erfindung offensichtlich sind, werden als im Geist und Umfang der Erfindung liegend betrachtet.

ZUSAMMENFASSUNG

[0062] Das Liefern eines Direct-Proof-Privatschlüssels an eine Vorrichtung, die in einem Clientcomputersystem im Feld installiert ist, kann in einer sicheren Weise erreicht werden, ohne daß ein signifikanter nichtflüchtiger Speicher in der Vorrichtung benötigt wird. Ein eindeutiger pseudozufälliger Wert wird erzeugt und zum Zeitpunkt der Herstellung in der Vorrichtung gespeichert. Der pseudozufällige Wert wird benutzt, um einen symmetrischen Schlüssel zum Verschlüsseln einer Datenstruktur zu erzeugen, die einen Direct-Proof-Privatschlüssel und einen Privatschlüsselextrakt enthält, die der Vorrichtung zugeordnet sind. Die resultierende verschlüsselte Datenstruktur wird auf einem entnehmbaren Speichermedium (wie z.B. einer CD) gespeichert und an den Eigentümer des Clientcomputersystems verteilt. Wenn die Vorrichtung auf dem Clientcomputersystem initialisiert wird, prüft das System, ob eine lokalisierte verschlüsselte Datenstruktur in dem System vorhanden ist. Wenn nicht, erhält das System die zugeordnete verschlüsselte Datenstruktur von dem entnehmbaren Speichermedium. Die Vorrichtung entschlüsselt die verschlüsselte Datenstruktur mit Hilfe eines symmetrischen Schlüssels, der aus seinem gespeicherten pseudozufälligen Wert regeneriert wurde, um den Direct-Proof-Privatschlüssel zu erhalten. Wenn der Privatschlüssel gültig ist, kann er von der Vorrichtung in dem Clientcomputersystem für eine nachfolgende Authentifizierungsverarbeitung benutzt werden.

Patentansprüche

1. Verfahren, das umfaßt:
Erzeugen einer verschlüsselten Datenstruktur, die einer Vorrichtung zugeordnet ist, wobei die verschlüsselte Datenstruktur einen Privatschlüssel und einen Privatschlüssel-Digest umfaßt;
Erzeugen eines Kennzeichners anhand eines pseudozufällig erzeugten Werts für die verschlüsselte Datenstruktur;
Speichern des Kennzeichners und der verschlüsselten Datenstruktur auf einem entnehmbaren Speichermedium; und
Speichern des pseudozufälligen Werts in einem nichtflüchtigen Speicher in der Vorrichtung.

2. Verfahren nach Anspruch 1, die ferner ein Verteilen des entfernbaren Speichermediums und der Vorrichtung umfaßt.

3. Verfahren nach Anspruch 1, die ferner ein Erzeugen eines Direct-Proof-Familienschlüsselpaars für eine Klasse von Vorrichtungen umfaßt.

4. Verfahren nach Anspruch 3, wobei der Privatschlüssel einen Direct-Proof-Privatschlüssel umfaßt, der einem öffentlichen Schlüssel des Direct-Proof-Familienschlüsselpaars zugeordnet ist,

wobei das Verfahren ferner ein Streuen des Direct-Proof-Privatschlüssels, um den Privatschlüssel-Digest zu erzeugen, umfaßt.

5. Verfahren nach Anspruch 1, das ferner ein Erzeugen eines symmetrischen Schlüssels anhand des pseudozufälligen Werts für die Vorrichtung umfaßt.

6. Verfahren nach Anspruch 5, wobei das Erzeugen des Kennzeichners ein Verschlüsseln eines Datenwerts unter Benutzung des symmetrischen Schlüssels umfaßt.

7. Verfahren nach Anspruch 5, das ferner ein Verschlüsseln der Datenstruktur unter Benutzung des symmetrischen Schlüssels umfaßt.

8. Verfahren nach Anspruch 1, wobei die verschlüsselte Datenstruktur außerdem einen zufälligen Initialisierungsvektor umfaßt.

9. Verfahren nach Anspruch 1, wobei das entnehmbare Speichermedium eine CD umfaßt.

10. Verfahren nach Anspruch 1, wobei der pseudozufällige Wert für die Vorrichtung eindeutig ist.

11. Gegenstand, der umfaßt: ein erstes Speichermedium, das mehrere maschinenlesbare Befehle aufweist, wobei, wenn die Befehle von einem Prozessor ausgeführt werden, die Befehle das Liefern von Privatschlüsseln an Vorrichtungen durch die folgenden Schritte vorsehen in:
Erzeugen einer verschlüsselten Datenstruktur, die einer Vorrichtung zugeordnet ist, und die einen Privatschlüssel und einen Privatschlüssel-Digest umfaßt;
Erzeugen eines Kennzeichners anhand eines pseudozufällig erzeugten Werts für die verschlüsselte Datenstruktur;
Speichern des Kennzeichners und der verschlüsselten Datenstruktur auf einem zweiten entnehmbaren Speichermedium; und
Veranlassen der Speicherung des pseudozufälligen Werts in nichtflüchtigem Speicher in der Vorrichtung.

12. Gegenstand nach Anspruch 11, der außerdem Befehle zum Erzeugen eines Direct-Proof-Familienschlüsselpaars für eine Klasse von Vorrichtungen umfaßt.

13. Gegenstand nach Anspruch 12, wobei der Privatschlüssel einen Direct-Proof-Privatschlüssel umfaßt, der einem öffentlichen Schlüssel des Direct-Proof-Familienschlüsselpaars zugeordnet ist, und außerdem Befehle zum Streuen des Direct-Proof-Familienschlüssels umfaßt, um den Privatschlüssel-Digest zu erzeugen.

14. Gegenstand nach Anspruch 11, der außerdem Befehle zum Erzeugen eines symmetrischen Schlüssels anhand des pseudozufälligen Werts für die Vorrichtung umfaßt.

15. Gegenstand nach Anspruch 14, wobei Befehle zum Erzeugen des Kennzeichners Befehle zum Verschlüsseln eines Datenwerts unter Benutzung des symmetrischen Schlüssels umfassen.

16. Gegenstand nach Anspruch 14, der außerdem Befehle zum Verschlüsseln der Datenstruktur unter Benutzung des symmetrischen Schlüssels umfaßt.

17. Gegenstand nach Anspruch 11, wobei die verschlüsselte Datenstruktur außerdem einen zufälligen Initialisierungsvektor umfaßt.

18. Gegenstand nach Anspruch 11, wobei der pseudozufällige Wert für die Vorrichtung eindeutig ist.

19. Verfahren, das umfaßt:
Bestimmen, ob eine verschlüsselte Datenstruktur, die einen Privatschlüssel und einen Privatschlüssel-Digest umfaßt und die einer Vorrichtung zugeordnet ist, die in einem Computersystem installiert ist, in einem Speicher des Computersystems gespeichert ist;
Deaktivieren der Funktion eines Schlüsselbeschaffungsbefehls, wenn die verschlüsselte Datenstruktur gespeichert ist;
Erhalten der verschlüsselten Datenstruktur, die der Vorrichtung zugeordnet ist, von einem entnehmbaren Speichermedium, auf das das Computersystem zugreifen kann, wobei auf dem entnehmbaren Speichermedium eine Datenbank mit verschlüsselten Datenbankstrukturen gespeichert ist, wenn die verschlüsselte Datenstruktur nicht gespeichert ist.

20. Verfahren nach Anspruch 19, wobei das entnehmbare Speichermedium eine CD umfaßt, die von einem Hersteller der Vorrichtung erstellt wurde.

21. Vorrichtung nach Anspruch 19, wobei das Erhalten der verschlüsselten Datenstruktur ein Ausstellen des Schlüsselerhaltbefehls an die Vorrichtung umfaßt, um einen Privatschlüsselbeschaffungsprozeß zu initiieren.

22. Verfahren nach Anspruch 19, wobei der Privatschlüssel einen Direct-Proof-Privatschlüssel umfaßt, der einem öffentlichen Schlüssel eines Direct-Proof-Familienschlüsselpaars für eine Klasse von Vorrichtungen zugeordnet ist.

23. Verfahren nach Anspruch 21, wobei der Privatschlüsselbeschaffungsprozeß ein Erzeugen eines symmetrischen Schlüssels anhand eines eindeutigen pseudozufälligen Werts umfaßt, der in der Vorrichtung gespeichert ist.

24. Verfahren nach Anspruch 23, wobei der Pri-

vatschlüsselbeschaffungsprozeß ein Erzeugen eines Vorrichtungskennzeichners anhand des pseudozufälligen Werts für die verschlüsselte Datenstruktur umfaßt.

25. Verfahren nach Anspruch 24, wobei der Privatschlüsselbeschaffungsprozeß außerdem umfaßt: Durchsuchen des entnehmbaren Speichermediums nach einem Eintrag in der Datenbank mit verschlüsselten Datenstrukturen, der durch einen Kennzeichner indexiert ist, der mit dem erzeugten Vorrichtungskennzeichner übereinstimmt, und Übertragen der verschlüsselten Datenstruktur an die Vorrichtung.

26. Vorrichtung nach Anspruch 25, wobei der Privatschlüsselbeschaffungsprozeß außerdem umfaßt: Entschlüsseln der verschlüsselten Datenstruktur, die von dem entnehmbaren Speichermedium empfangen wurde, unter Benutzung des symmetrischen Schlüssels, um den Privatschlüssel und den Privatschlüssel-Digest zu erhalten.

27. Verfahren nach Anspruch 26, wobei der Privatschlüsselbeschaffungsprozeß außerdem umfaßt: Streuen des Privatschlüssels, um einen neuen Privatschlüssel-Digest zu erzeugen, Vergleichen des Privatschlüssel-Digests von der entschlüsselten Datenstruktur mit dem neuen Privatschlüssel-Digest, und Akzeptieren des Privatschlüssels als gültig für die Vorrichtung, wenn die Digests übereinstimmen.

28. Gegenstand, der umfaßt: ein erstes Speichermedium, das mehrere maschinenlesbare Befehle aufweist, wobei, wenn die Befehle von einem Prozessor ausgeführt werden, die Befehle das Erhalten eines Privatschlüssels für eine Vorrichtungen, die in einem Computersystem installiert ist, durch die folgenden Schritte vorsehen:
Bestimmen, ob eine verschlüsselte Datenstruktur, die den Privatschlüssel und einen Privatschlüssel-Digest umfaßt und die der Vorrichtung zugeordnet ist, die in dem Computersystem installiert ist, in einem Speicher des Computersystems gespeichert ist;
Deaktivieren der Funktion eines Schlüsselbeschaffungsbefehls, wenn die verschlüsselte Datenstruktur gespeichert ist;
Erhalten der verschlüsselten Datenstruktur, die der Vorrichtung zugeordnet ist, von einem entnehmbaren Speichermedium, auf das das Computersystem zugreifen kann, wobei auf dem entnehmbaren Speichermedium eine Datenbank aus verschlüsselten Datenstrukturen gespeichert ist, wenn die verschlüsselte Datenstruktur nicht gespeichert ist.

29. Gegenstand nach Anspruch 28, wobei Befehle zum Erhalten der verschlüsselten Datenstruktur Befehle zum Ausstellen des Schlüsselbeschaffungsbefehls an die Vorrichtung umfassen, um einen Privatschlüsselbeschaffungsprozeß zu initialisieren.

30. Gegenstand nach Anspruch 28, wobei der Privatschlüssel einen Direct-Proof-Privatschlüssel umfaßt, der einem öffentlichen Schlüssel eines Direct-Proof-Familienschlüsselpaars für eine Klasse von Vorrichtungen zugeordnet ist.

31. Gegenstand nach Anspruch 29, wobei der Privatschlüsselbeschaffungsprozeß Befehle zum Erzeugen eines symmetrischen Schlüssels anhand eines eindeutigen pseudozufälligen Werts umfaßt, der in der Vorrichtung gespeichert ist.

32. Gegenstand nach Anspruch 31, wobei der Privatschlüsselbeschaffungsprozeß Befehle zum Erzeugen eines Vorrichtungskennzeichners anhand des pseudozufälligen Werts für die verschlüsselte Datenstruktur umfaßt.

33. Gegenstand nach Anspruch 32, wobei der Privatschlüsselbeschaffungsprozeß Befehle zum Durchsuchen des entnehmbaren Speichermediums nach einem Eintrag in der Datenbank mit verschlüsselten Datenbankstrukturen umfaßt, der durch einen Kennzeichner indexiert ist, der mit dem erzeugten Vorrichtungskennzeichner übereinstimmt, und zum Übertragen der verschlüsselten Datenstruktur an die Vorrichtung.

34. Gegenstand nach Anspruch 33, wobei der Privatschlüsselbeschaffungsprozeß außerdem Befehle zum Entschlüsseln der verschlüsselten Datenstruktur umfaßt, die von dem entnehmbaren Speichermedium empfangen wurde, unter Benutzung des symmetrischen Schlüssels, um den Privatschlüssel und den Privatschlüssel-Digest zu erhalten.

35. Gegenstand nach Anspruch 34, wobei der Privatschlüsselbeschaffungsprozeß außerdem Befehle zum Streuen des Privatschlüssels, um einen neuen Privatschlüssel-Digest zu erzeugen, zum Vergleichen des Privatschlüssel-Digests von der entschlüsselten Datenstruktur mit dem neuen Privatschlüssel-Digest, und zum Akzeptieren des Privatschlüssels als gültig für die Vorrichtung umfaßt, wenn die Digests übereinstimmen.

36. Verfahren, das umfaßt:
Abrufen einer verschlüsselten Datenstruktur, die einen Privatschlüssel und einen Privatschlüssel-Digest umfaßt und die einer Vorrichtung zugeordnet ist, die in einem Computersystem installiert ist, aus einem Speicher in dem Computersystem;
Erzeugen eines symmetrischen Schlüssels anhand eines eindeutigen pseudozufälligen Werts, der in der Vorrichtung gespeichert ist;
Entschlüsseln der verschlüsselten Datenstruktur unter Benutzung des symmetrischen Schlüssels, um den Privatschlüssel und den Privatschlüssel-Digest zu erhalten;
Streuen des Privatschlüssels, um einen neuen Pri-

vatschlüssel-Digest zu erzeugen, und Vergleichen des Privatschlüssels aus der entschlüsselten Datenstruktur mit dem neuen Privatschlüssel-Digest; und
Akzeptieren des Privatschlüssels als gültig für die Vorrichtung, wenn die Digests übereinstimmen.

37. Verfahren nach Anspruch 36, wobei der Privatschlüssels einen Direct-Proof-Privatschlüssel umfaßt, der einem öffentlichen Schlüssel eines Direct-Proof-Familienschlüsselpaars für eine Klasse von Vorrichtungen zugeordnet ist.

38. Verfahren nach Anspruch 36, wobei die Vorrichtung eine Peripherievorrichtung des Computersystems umfaßt.

39. Verfahren nach Anspruch 36, das ferner umfaßt:
Erzeugen eines zufälligen Initialisierungsvektors;
Erzeugen einer neuen verschlüsselten Datenstruktur durch Verschlüsseln des Privatschlüssels, des Privatschlüssel-Digests und des zufälligen Initialisierungsvektors unter Benutzung des symmetrischen Schlüssels; und
Speichern der neuen verschlüsselten Datenstruktur in dem Speicher des Computersystems.

Es folgt kein Blatt Zeichnungen